IN THE CLAIMS:

1. (Previously Presented) A method, comprising:

receiving, in a secure environment in a terminal, via a secure channel, from a server outside said terminal, a first key for decrypting an encrypted application;

decrypting, in the secure environment, said encrypted application by means of said first key;

re-encrypting, in said secure environment, the application by means of a second key; and

storing, outside said secure environment, the re-encrypted application.

2. (Previously Presented) A method, comprising:

receiving an encrypted application in a terminal;

receiving, in a secure environment in said terminal, via a secure channel, from a server outside said terminal, a first key for decrypting said encrypted application;

encrypting, in said secure environment, said first key by means of a second key; and

storing, outside said secure environment, the encrypted first key.

3. (Previously Presented) The method according to claim 1, the method comprising:

encrypting, in said secure environment, said first key by means of the second key; and

storing, outside said secure environment, the encrypted first key.

4. (Previously Presented) The method according to claim 1, wherein said second key is symmetric and can be derived from the application.

5. (Previously Presented) The method according to claim 4, wherein said second key is comprised in the application itself.

6. (Previously Presented) The method according to claim 4, wherein said second key is generated in the secure environment using an application seed.

7. (Original) The method according to claim 1, wherein multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

8. (Previously Presented) Apparatus, comprising:

an application including an installation part for receiving, in a secure environment of a terminal, via a secure channel, from a server outside said terminal, a first key for decrypting an encrypted application;

a processor for decrypting, in the secure environment, said encrypted application by means of said first key;

said processor for re-encrypting, in said secure environment, the application based on a second key; and

a memory for storing, outside said secure environment, the re-encrypted application.

9. (Previously Presented) Apparatus, comprising:

an application including an installation part for receiving, in a secure environment of a terminal, via a secure channel, from a server outside said terminal, a first key for decrypting an encrypted application;

a processor for encrypting, in said secure environment, said first key by means of a second key; and

said processor for storing in a memory of said terminal, outside said secure environment, the encrypted first key.

10. (Previously Presented) The apparatus according to claim 8, wherein said processor is:

for encrypting, in said secure environment, said first key by means of the second key; and

for storing, outside said secure environment, the encrypted first key.

11. (Previously Presented) The apparatus according to claim 8, wherein said second key is symmetric and can be derived from the application.

12. (Previously Presented) The apparatus according to claim 11, wherein said second key is comprised in the application itself.

13. (Previously Presented) The apparatus according to claim 11, wherein said second key is generated in the secure environment using an application seed.

14. (Previously Presented) The apparatus according to claim 8, wherein the apparatus is arranged such that multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

15. (Previously Presented) The method of claim 2, wherein said second key is symmetric and can be derived from the application.

16. (Previously Presented) The method of claim 15, wherein said second key is comprised in the application itself.

17. (Previously Presented) The method of claim 15, wherein said second key is generated in the secure environment using an application seed.

18. (Original) The method of claim 2, wherein multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

19. (Previously Presented) The method of claim 9, wherein said second key is symmetric and can be derived from the application.

20. (Previously Presented) The method of claim 19, wherein said second key is comprised in the application itself.

21. (Previously Presented) The method of claim 9, wherein the apparatus is arranged such that multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

22. (Previously Presented) A terminal device comprising:

an installation part of an application, responsive to a first key provided over a secure channel from a server external to said terminal device for providing said first key; and

a secure environment, responsive to said first key from said installation part of said application for decrypting an encrypted application in said terminal device using said first key received over said secure channel from said server external to said terminal device.

23. (Previously Presented) The terminal device of claim 22, wherein said first key is encrypted by said server using a second key belonging to said terminal device for providing said first key from said server to said terminal device.

24. (Previously Presented) An integrated circuit for installation in a terminal comprising a signal processor and a secure environment, said secure environment responsive to a first key from a server outside said terminal received over a secure channel for decrypting an encrypted application within said secure environment, for executing said decrypted application within said secure environment and for encrypting said first key with a second key belonging to said terminal device for storage outside said secure environment so that said first key can be used again

within said secure environment without need for receipt again of said first key from said server.

25. (New) The method of claim 2, further comprising

receiving another encrypted application in the terminal;

loading the encrypted first key from outside said secure environment;

decrypting the encrypted first key with the second key; and

decrypting the other encrypted application with the decrypted first key.

26. (New) The method of claim 25, further comprising:

re-encrypting the first key by means of the second key; and

storing, outside said secure environment, the encrypted first key.

27. (New) The apparatus of claim 9, wherein said installation part is for receiving another encrypted application in the terminal and wherein said processor is configured to:

load the encrypted first key from outside said secure environment;

decrypt the encrypted first key with the second key; and

decrypt the other encrypted application with the decrypted first key.

28. (New) The apparatus of claim 27, wherein said processor is further configured to:

re-encrypt the first key by means of the second key; and

store, outside said secure environment, the encrypted first key.

29. (New) The method of claim 7, further comprising:

encrypting, in said secure environment, each of said multiple keys by means of the second key; and

storing, outside said secure environment, each of the multiple keys encrypted by the second key.

30. (New) The method of claim 29, further comprising:

receiving a plurality of encrypted applications in the terminal and storing same outside said secure environment;

loading one of said plurality of encrypted applications into the secure environment;

loading a corresponding one of said plurality of encrypted multiple keys stored outside said secure environment into said secure environment;

decrypting the corresponding encrypted key by means of the second key; and

decrypting the loaded encrypted application by means of the decrypted corresponding key.

31. (New) The apparatus of claim 14, wherein said processor is configured to:

encrypt, in said secure environment, each of said multiple keys by means of the second key; and

store, outside said secure environment, each of the multiple keys encrypted by the second key.

32. (New) The apparatus of claim 31, wherein said apparatus is configured to:

receive a plurality of encrypted applications;

to store same outside said secure environment;

to load a selected one of said plurality of encrypted applications into the same environment;

load a corresponding one of said plurality of encrypted multiple keys stored outside said secure environment into said secure environment;

decrypt the corresponding encrypted key by means of the second key; and

decrypt the loaded selected encrypted application by means of the decrypted corresponding key.